修 士 論 文 の 和 文 要 旨

大学院情報システム学研究科　博士前期課程　情報ネットワーク学専攻		
氏　　名	岩崎 泰隆	学籍番号　0551006
論 文 題 目	Peres法によるユニバーサル乱数生成アルゴリズムの拡張とその性能評価	

要　旨

計算機が登場する前は，乱数は国勢調査報告書の中などから適当に数値を抜き出し，乱数表を作成し，そこから利用していた．ところが計算機の登場によりこの方法は次第に使われなくなり，代わりに擬似乱数を作り出す方法を求める試みがなされるようになった．

いままで擬似乱数生成法としては，いろいろと提案されてきたが，特に乱数生成“アルゴリズム”という概念が，1946年頃にJohn von Neumannによって初めて提案され，研究者の脚光をあびるようになった．続いて，1948年頃にD.H.Lehmerによって線形合同法と呼ばれる乱数生成法が考案され，今日でも広く用いられている．しかしこの方法ではいくつかの問題点が指摘されており，それに変わるものとしてM系列と呼ばれる手法が考案された．現在では，M系列をさらに改良した，松本らによるメルセンヌ・ツイスタ法が，現段階では“最適”な擬似乱数を生成すると思われており，現在広い分野で用いられている．ところがここで挙げた擬似乱数生成法はすべて“線形漸化式”によって生成されるため，予測可能であるという欠陥を免れない．そこで，線形漸化式によらない乱数生成器の開発が求められている．

一方，ある「確率分布が未知」で定常無記憶な情報源（ユニバーサル情報源という）から，任意の情報源に従う乱数列を生成する，原理上は予測不可能なアルゴリズムが1951年，John von Neumannによって提案されたが，これは無駄が多く効率が悪かった．その後も数々の研究が行われ，1993年には，Yuval Peresにより，定常な無記憶情報源を用いて作成した可変長乱数列の平均長がエントロピーレートに漸近することを保証する，“Iterating-von-Neumann-procedure” という漸近最適な手法が提案された．そこで本研究ではこの手法を実際に計算機上でシミュレーションを行うことにより，その性質を考察する．さらに，任意のk次マルコフ定常乱数列(確率分布は未知)から，偏りのないコイン(定常無記憶乱数列)を作るアルゴリズムに拡張することを考える(ユニバーサルな乱数生成)．